

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-039795**

(43)Date of publication of application : 12.02.1999

(51)Int.CI.

G11B 20/10

G06F 12/14

G09C 1/00

H04L 9/16

H04L 9/36

(21)Application number : 09-186837

(71)Applicant : **TOSHIBA CORP**

(22)Date of filing : 11.07.1997

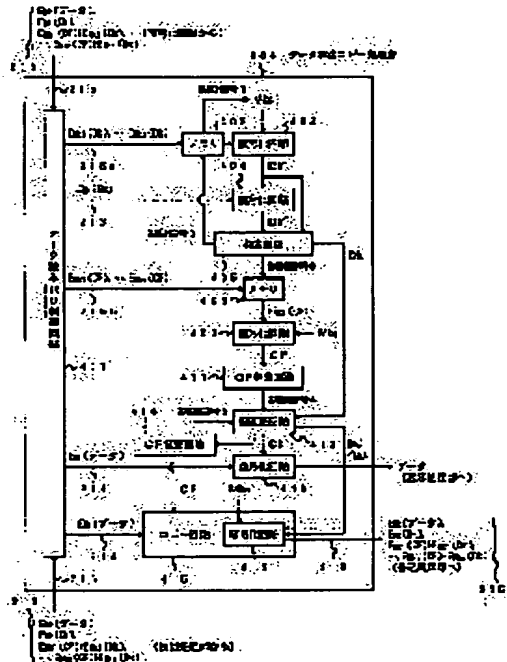
(72)Inventor : **KATO TAKEHISA**

(54) DEVICE FOR PREVENTING UNAUTHORIZED DATA COPY AND METHOD THEREFOR AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To surely protect an attack of an unauthorized person against a part under copy management in data.

SOLUTION: In this device to be used for equipment for copying digital data, the digital data 215 has an enciphered data itself EDk and enciphered copy management information (EMk1(CF)+EMk1(Dk),..., EMkn(CF)+EMkn(Dk)) for managing approval of copying this data itself EDk. When the digital data is judged to be disapproval of its copy, provided contents of this copy management information are satisfied with prescribed conditions (411), the digital data is not copied at all (412).



LEGAL STATUS

[Date of request for examination]

18.09.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

- [Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-39795

(43)公開日 平成11年(1999)2月12日

(51)Int.Cl. ^o	識別記号	F I
G 1 1 B 20/10		G 1 1 B 20/10 H
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14 3 2 0 E
		3 2 0 B
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00 6 6 0 D
H 0 4 L 9/16		H 0 4 L 9/00 6 4 3

審査請求 未請求 請求項の数10 O.L (全 22 頁) 最終頁に続く

(21)出願番号 特願平9-186837

(22)出題日 平成9年(1997)7月11日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 加藤 岳久

東京都府中市東芝町1番地 株式会社東芝
府中工場内

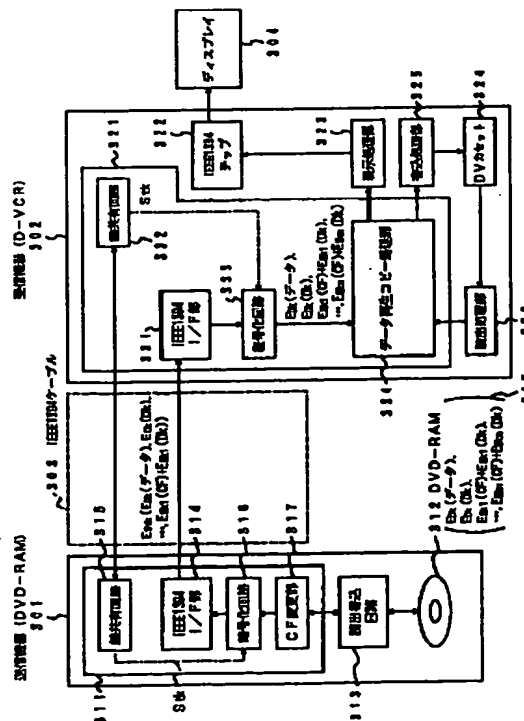
(74)代理人 弁理士 鈴江 武彦 (外6名)

(54)【発明の名称】 不正データコピー防止装置及び方法並びに記録媒体

(57) 【要約】

【課題】 データ内のコピー管理を行う部分に対する不正者の攻撃を確実に防御できる。

【解決手段】 デジタルデータをコピーする機器に用いられる不正データコピー防止装置において、デジタルデータ 215 は、暗号化されたデータ本体 214 と、当該データ本体のコピー許可について管理する暗号化されたコピー管理情報 212 と有し、コピー管理情報の内容が所定の条件を満たして、デジタルデータがコピー不許可と判定されたとき（411）には、デジタルデータのコピーを行わない（412）不正データコピー防止装置。



【特許請求の範囲】

【請求項1】 デジタルデータをコピーする機器に用いられる不正データコピー防止装置において、前記デジタルデータは、暗号化されたデータ本体と、当該データ本体のコピー許可について管理する暗号化されたコピー管理情報とを有し、前記コピー管理情報の内容が所定の条件を満たして、前記デジタルデータがコピー不許可と判定されたときには、前記デジタルデータのコピーを行わないことを特徴とする不正データコピー防止装置。

【請求項2】 デジタルデータをコピーする機器に用いられる不正データコピー防止装置において、前記デジタルデータは、暗号化されたデータ本体と、当該データ本体のコピー許可について管理する暗号化されたコピー管理情報と、前記データ本体を復号するための鍵情報とを有し、前記コピー管理情報の内容が所定の条件を満たして、前記デジタルデータがコピー不許可と判定されたときには、前記デジタルデータ内の前記鍵情報を変更する鍵変更手段を備えたことを特徴とする不正データコピー防止装置。

【請求項3】 前記コピー管理情報は、前記デジタルデータが最初のデータから何回目のコピーであるかを示す世代管理情報と、当該デジタルデータを何回コピーしたかを示すコピー回数管理情報からなり、前記世代管理情報が所定の世代数となり、前記コピー回数管理情報が所定のコピー回数となると、コピー不許可であることを示す請求項1又は2記載の不正データコピー防止装置。

【請求項4】 前記コピー管理情報は、前記デジタルデータが最初のデータから何回目のコピーであるかを示す世代管理情報を有し、当該世代管理情報が所定の世代数となるとコピー不許可であることを示すものであり、かつ、その情報ビット数を3ビット以上として、最初のデータのコピーのコピー以上の世代のデータまでコピー許可管理可能としたことを特徴とする請求項1又は2記載の不正データコピー防止装置。

【請求項5】 前記デジタルデータを送信機器と受信機器間で伝送する場合であり、かつ前記送信機器又は前記受信機器に適用される不正データコピー防止装置であって、前記送信機器と前記受信機器と間で共有された一時鍵を暗号鍵もしくは復号鍵として、両者間で伝送される前記デジタルデータを暗号化もしくは復号化する暗号化手段もしくは復号化手段を備えたことを特徴とする請求項1乃至4のうち何れか1項記載の不正データコピー防止装置。

【請求項6】 デジタルデータをコピーする機器に用いられる不正データコピー防止方法において、前記デジタルデータは、暗号化されたデータ本体と、当該データ本体のコピー許可について管理する暗号化されたコピー管理情報と、前記データ本体を復号するための鍵情報とを有し、前記コピー管理情報の内容が所定の条件を満たして、前記デジタルデータがコピー不許可と判定されたときには、前記デジタルデータ内の前記鍵情報を変更することを特徴とする不正データコピー防止方法。

【請求項7】 デジタルデータをコピーする機器に用いられる不正データコピー防止方法において、前記デジタルデータが最初のデータから何回目のコピーであるかを示す世代管理情報と、当該デジタルデータを何回コピーしたかを示すコピー回数管理情報からなるコピー管理情報を前記デジタルデータに付加し、前記世代管理情報が所定の世代数となり、前記コピー回数管理情報が所定のコピー回数となると、コピー不許可として不正なデータコピーを防止することを特徴とする不正データコピー防止方法。

【請求項8】 暗号化されたデータ本体と、当該データ本体のコピー許可について管理する暗号化されたコピー管理情報と、前記データ本体を復号するための鍵情報と、前記コピー管理情報を復号するための鍵情報とを有するデータ構造体が記録されたコンピュータ読み取り可能な記録媒体。

【請求項9】 暗号化されたデータ本体と、前記データ本体を復号するためのデータ暗号鍵が当該データ暗号鍵を暗号鍵として暗号化されてなる第1の鍵情報と、前記データ暗号鍵が複数の暗号鍵によりそれぞれ暗号化されてなる複数の第2の鍵情報と、前記データ本体のコピー許可について管理するコピー管理情報が、前記複数の暗号鍵によりそれぞれ暗号化されてなる複数の第3の鍵情報とを有するデータ構造体が記録されたコンピュータ読み取り可能な記録媒体。

【請求項10】 暗号化されたデータ本体と、前記データ本体を復号するためのデータ暗号鍵が当該データ暗号鍵を暗号鍵として暗号化されてなる第1の鍵情報と、前記データ暗号鍵が複数の暗号鍵によりそれぞれ暗号化されてなる複数の第2の鍵情報と、前記データ本体のコピー許可について管理するコピー管理情報が、前記データ暗号鍵を暗号鍵として暗号化されてなる第3の鍵情報とを有するデータ構造体が記録されたコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明はデータコピー防止装置及び方法並びに記録媒体、特にデジタル化された文書、音声、画像、プログラム等のデータを不正にコピーすることを防止する不正データコピー防止装置及び方法並びに記録媒体に関するものである。

【0002】

【従来の技術】近年、デジタル記録再生機器の開発、製品化が進み、これらのデジタル記録再生機器間で画質や音質の劣化なくデータをコピーすることが可能となっている。しかし高画質な複製は、海賊版と呼ばれる不正なコピーを増加させ、著作権が侵害されるという問題がある。このような不正なコピーは確実に防止されなければならない。というのも、D-VCRやDVD-RAM等の大容量デジタル記録再生機器の出現により、デジタル化された著作物は簡単にコピーされ、不特定多数への配布が可能となり、これによりデジタル画像等の著作権者に危機感を与えているからである。

【0003】不正コピーを行う手段としては種々の方法が考えられるが、とにかく不正者はDVD-ROMドライブやD-VCRといった再生装置等の機器からコピー対象とするデータを受け取り、DVD-RAM等の他のデジタル記録機器で複写するという手続きを踏む必要がある。

【0004】従来のDVD等ほど大容量でないデジタル記録再生機器、例えばDATやMDでは、その不正なデータコピーを防止する手段として、SCMS（シリアルコピーマネージメントシステム）を用いている。

【0005】SCMSでは、例えばCDからMD（又はDAT）へ、もしくはMD（又はDAT）からMD（又はDAT）へのデータコピーを行うに当たり、そのデータヘッドにコピー情報が付加されている。このコピー情報は2ビットからなるデータで、マスターディスクにおけるコピー情報が“00”の場合は、コピーを取ってもコピー情報は“00”のままであり、自由なコピーが可能である。

【0006】一方、マスターディスクにおけるコピー情報が“10”の場合は、子供のコピー（例えば、マスターディスクから一代下のディスクのコピー）は可能であるが、孫のコピー（例えば、マスターディスクから二世世代下のディスクのコピー）は不可能である。つまり、この場合は、コピーの際、このコピー情報がカウントアップされて“11”となる。これが子供のコピーである。そして各システムはコピー情報が“11”の場合はコピーできないように構成されており、孫のコピーを防止するようになっている。

【0007】以上のシステムは、著作権保護のための不正なコピーを防止すべく構成された正当な機器を使用した場合の不正コピー防止方法である。しかし、各機器に不正コピー防止の対策が施されていても、機器間でデータを転送する際にその伝送路上で不正者によりデータが

横流しされてしまったのでは、上記対策も無意味なものとなる。

【0008】このような場合に対応し、従来から秘密性を要するデータを通信する際には、これを暗号化して送信することが広く行われている。暗号化方式には、大きく別けて公開鍵方式と秘密鍵方式があるが、上記場合のように処理の高速性が要求されるときは、秘密鍵を用いるのが一般的である。この秘密鍵を用いて暗号化を行う場合には、予めどの秘密鍵を用いて暗号化を行うか、通信者間で決めておき特定の秘密鍵を用いて暗号通信を行っている。

【0009】

【発明が解決しようとする課題】このため秘密鍵が第三者に、例えば攻撃による秘密鍵の特定による盗用などによる漏洩があると、それが発覚した場合に、再度使用する秘密鍵を通信者間で更新する必要がある。したがって、より有効な機器間伝送における暗号化の方式が要望されている。

【0010】また、不当なコピーデータに対しては、これを有効に再生させないような仕組みが必要である。また、上記SCMSによる不正コピーの管理では、子供のコピーはいくらでも取れるので、子供のコピーからのコピー（孫コピー）をとることはできなくとも、悪意の不正者により子供のコピーが大量に作成される場合がある。さらに、SCMSでは、コピー情報自体が不正者によって例えば“00”に書き換えられると、以降の不正コピーは自由に行われることになる。

【0011】したがって、著作権の問題がさらに深刻となる大容量デジタル記録再生機器の場合には、SCMSよりも確実に、かつ、きめ細かなコピー管理を実現可能なコピー管理方法が求められている。

【0012】本発明は、このような実情を考慮してなされたもので、その第1の目的は、データ内のコピー管理を行う部分に対する不正者の攻撃を確実に防御できる不正データコピー防止装置及び方法並びに記録媒体を提供することにある。

【0013】また、第2の目的は、不正なコピーデータを有効に再生させないようにする不正データコピー防止装置及び方法を提供することにある。さらに、第3の目的は、きめ細かなコピー管理を実現可能な不正データコピー防止装置及び方法を提供することにある。

【0014】

【課題を解決するための手段】上記課題を解決するために、請求項1に対応する発明は、デジタルデータをコピーする機器に用いられる不正データコピー防止装置において、デジタルデータは、暗号化されたデータ本体と、当該データ本体のコピー許可について管理する暗号化されたコピー管理情報と有し、コピー管理情報の内容が所定の条件を満たして、デジタルデータがコピー不許可と判定されたときには、デジタルデータのコピーを行わな

い不正データコピー防止装置である。

【0015】本発明はこのような手段を設けたので、データ内のコピー管理を行う部分、すなわちコピー管理情報に対する不正者の攻撃を確実に防御することができる。また、請求項2又は6に対応する発明は、デジタルデータをコピーする機器に用いられる不正データコピー防止装置又は方法において、デジタルデータは、暗号化されたデータ本体と、当該データ本体のコピー許可について管理する暗号化されたコピー管理情報と、データ本体を復号するための鍵情報とを有し、コピー管理情報の内容が所定の条件を満たして、デジタルデータがコピー不許可と判定されたときには、デジタルデータ内の鍵情報を変更する鍵変更手段を備えた不正データコピー防止装置又は方法である。

【0016】本発明はこのような手段を設けたので、不正なコピーデータを有効に再生させないようにすることができる。すなわちデジタルデータがコピー不許可と判定されたときには、デジタルデータ内の鍵情報を変更され、そのコピーされたデジタルデータは有効な再生ができないことになる。

【0017】さらに、請求項3に対応する発明は、請求項1又は2に対応する発明において、コピー管理情報は、デジタルデータが最初のデータから何回目のコピーであるかを示す世代管理情報と、当該デジタルデータを何回コピーしたかを示すコピー回数管理情報からなり、世代管理情報が所定の世代数となり、コピー回数管理情報が所定のコピー回数となると、コピー不許可であることを示す不正データコピー防止装置である。

【0018】本発明はこのような手段を設けたので、請求項1又は2に対応する発明と同様な作用効果が得られる他、きめ細かなコピー管理を実現することができる。さらにまた、請求項4に対応する発明は、請求項1又は2に対応する発明において、コピー管理情報は、デジタルデータが最初のデータから何回目のコピーであるかを示す世代管理情報を有し、当該世代管理情報が所定の世代数となるとコピー不許可であることを示すものであり、かつ、その情報ビット数を3ビット以上として、最初のデータの複製のコピー以上の世代のデータまでコピー許可管理可能とした不正データコピー防止装置である。

【0019】本発明はこのような手段を設けたので、請求項1又は2に対応する発明と同様な作用効果が得られる他、きめ細かなコピー管理を実現することができる。一方、請求項5に対応する発明は、請求項1～4に対応する発明において、デジタルデータを送信機器と受信機器間で伝送する場合であり、かつ送信機器又は受信機器に適用される不正データコピー防止装置であって、送信機器と受信機器と間で共有された一時鍵を暗号鍵もしくは復号鍵として、両者間で伝送されるデジタルデータを暗号化もしくは復号化する暗号化手段もしくは復号化手

段を備えた不正データコピー防止装置である。

【0020】本発明はこのような手段を設けたので、請求項1～4に対応する発明と同様な作用効果が得られる他、たとえデジタルデータ自体がデータ伝送中に不正コピーされても、伝送中はさらに暗号化されているので、不正者の不正利用を防止することができる。

【0021】また、請求項7に対応する発明は、デジタルデータをコピーする機器に用いられる不正データコピー防止方法において、デジタルデータが最初のデータから何回目のコピーであるかを示す世代管理情報と、当該デジタルデータを何回コピーしたかを示すコピー回数管理情報からなるコピー管理情報をデジタルデータに付加し、世代管理情報が所定の世代数となり、コピー回数管理情報が所定のコピー回数となると、コピー不許可として不正なデータコピーを防止する不正データコピー防止方法である。

【0022】本発明はこのような手段を設けたので、きめ細かなコピー管理を実現することができる。次に、請求項8に対応する発明は、暗号化されたデータ本体と、当該データ本体のコピー許可について管理する暗号化されたコピー管理情報と、データ本体を復号するための鍵情報と、コピー管理情報を復号するための鍵情報とを有するデータ構造体が記録されたコンピュータ読み取り可能な記録媒体である。

【0023】本発明はこのような手段を設けたので、コピー管理情報に対する不正者の攻撃を確実に防御することができる。ここで、コンピュータ読み取り可能な、としているが、ここでのいうコンピュータはいわゆる計算機のみならず、デジタル再生記録機器等のあらゆる情報処理装置を含むものである。

【0024】また、請求項9に対応する発明は、暗号化されたデータ本体と、データ本体を復号するためのデータ暗号鍵が当該データ暗号鍵を暗号鍵として暗号化されてなる第1の鍵情報と、データ暗号鍵が複数の暗号鍵によりそれぞれ暗号化されてなる複数の第2の鍵情報と、データ本体のコピー許可について管理するコピー管理情報が、複数の暗号鍵によりそれぞれ暗号化されてなる複数の第3の鍵情報とを有するデータ構造体が記録されたコンピュータ読み取り可能な記録媒体である。

【0025】本発明はこのような手段を設けたので、コピー管理情報に対する不正者の攻撃をより一層確実に防御することができる。ここで、コンピュータ読み取り可能な、としているが、ここでのいうコンピュータはいわゆる計算機のみならず、デジタル再生記録機器等のあらゆる情報処理装置を含むものである。

【0026】さらに、請求項10に対応する発明は、暗号化されたデータ本体と、データ本体を復号するためのデータ暗号鍵が当該データ暗号鍵を暗号鍵として暗号化されてなる第1の鍵情報と、データ暗号鍵が複数の暗号鍵によりそれぞれ暗号化されてなる複数の第2の鍵情報

と、データ本体のコピー許可について管理するコピー管理情報が、データ暗号鍵を暗号鍵として暗号化されてなる第3の鍵情報とを有するデータ構造体が記録されたコンピュータ読み取り可能な記録媒体である。

【0027】本発明はこのような手段を設けたので、コピー管理情報に対する不正者の攻撃をより一層確実に防御することができる。ここで、コンピュータ読み取り可能な、としているが、ここでいうコンピュータはいわゆる計算機のみならず、デジタル再生記録機器等のあらゆる情報処理装置を含むものである。

【0028】

【発明の実施の形態】以下、本発明の実施の形態について説明する。本明細書では、暗号に関する技術について説明するが、以降、暗号化の操作を $Ey(x)$ と表す。ここで、 x は暗号化の対象となるデータで、 y は暗号化に用いる暗号鍵である。また復号化の操作を $Dy(z)$ と表す。ここで、 z は復号の対象となるデータで、 y は復号化に用いる復号鍵である。従って、

$$Ey(Dy(x))=x$$

$$Dy(Ey(x))=x$$

である。

【0029】また、本実施形態を説明する図において、一点鎖線は暗号化または復号化のための鍵情報を表し、実線は暗号化または復号化の対象となる情報を表している。

(発明の第1の実施の形態) 図1は本発明の第1の実施の形態に係る不正データコピー防止装置を適用するデジタル記録再生機器の接続構成例を示すブロック図である。

【0030】同図では、ケーブルテレビ網を利用して音声/画像/文字などのマルチメディア情報が配信され、STB(Set Top Box)101へ入力される例を示している。

【0031】このシステムは、STB101がIEEE1394ケーブル102を介してデジタルVCR103に接続されるとともに、デジタルVCR103からIEEE1394ケーブル104、105を介してそれぞれディスプレイ106とDVD-RAM107に接続され構成されている。同システムでは複数のデジタル記録再生機器が接続されているので、基本的には機器間でデータ送信、コピー等が可能である。

【0032】このシステムでは、STB101、デジタルVCR103又はDVD-RAM107がデータの送信機器になるものであり、一方、デジタルVCR103又はDVD-RAM107がデータの受信機器になるものである。本実施形態では、これら各送信機器、受信機器間での不正なデータコピーを防止する方法について説明する。

【0033】なお、上記構成について説明すると、まず、STB101はマルチメディアデータのスクランブ

ルを解いたり(あるいはデシャッフリング)課金情報などの蓄積/送信を行うためのものである。STB101へ入力されたマルチメディアデータは、IEEE1394ケーブル102、104、105を介して各機器103、106、107に接続されているが、IEEE1394とは高速シリアルデジタルインターフェースで、IEEEで制定されたものである。このインターフェースでは高速通信が可能で2種類のデータ転送、Asynchronous(非同期)とIsochronous(等時)ができる。このため、パーソナルコンピュータやデジタルテレビ、デジタルVCR、DVD-RAMなどのデジタルAV機器との接続に利用されるものである。

【0034】次に本実施形態の不正データコピー防止方法を実現するためのデータ構造について説明する。図2は本実施形態に使用されるデータ構造の構成方法を説明する図である。

【0035】DVD等に格納されるデータは、タイトルキーやディスクキーを用いてコンテンツを暗号化する。本実施形態では簡単化のためコンテンツはディスクキーと呼ばれるデータ暗号鍵 Dk で暗号化されることとする。図2において暗号化回路204によってデータがデータ暗号鍵 Dk で暗号化され EDk (データ)となる様子が示されている。このデータ暗号鍵 Dk は事前にデジタル記録再生機器製造メーカに知らされることはない。

【0036】また、デジタル記録再生機器において画像等のデータを再生すべく上記データ暗号鍵 Dk が暗号化されてデータ構造の一部として付加される。この暗号化されたデータ暗号鍵 Dk は2種類用意される。その1つはデータ暗号鍵 Dk 自体を暗号鍵としてデータ暗号鍵 Dk を暗号化するもので、暗号化回路203により当該暗号化され EDk (Dk)となる。もう1つは、データ暗号鍵 Dk をマスター鍵束 Mkn の各マスター鍵でそれぞれ暗号化する場合で、暗号化回路202により鍵束の鍵数だけ暗号化データ $EMk1(Dk)$ 、 $EMk2(Dk)$ 、...、 $EMkn(Dk)$ が生成される。

【0037】このマスター鍵束 Mkn は、例えば鍵管理会社によって管理されるものであり、デジタル記録再生機器製造メーカはこの鍵管理会社からマスター鍵束 Mkn の一部分であるマスター鍵束 Mks が与えられる。このマスター鍵束 Mks はメーカにより異なる複数個のマスター鍵からなるものであり、これにより鍵管理がなされることになる。すなわち各メーカはマスター鍵 $Mk1$ 、 $Mk2$ 、...、 Mkn のうち少なくともその一部を所有しているので、データ構造の中に暗号化データ $EMk1(Dk)$ 、 $EMk2(Dk)$ 、...、 $EMkn(Dk)$ と、 $EDk(Dk)$ とが含まれていれば、安全確実なデータ暗号鍵 Dk の取出しが可能になる。データ暗号鍵 Dk 取出方法の詳細は後述する。

【0038】本発明は、データコピーの安全な管理を行

うために、データ構造の中に、コピー管理フラグCFを暗号化して含めるようにしている。図2においてコピー管理フラグCFがマスター鍵束Mknによって暗号化回路201において暗号化され、暗号化データ列EMk1(CF), EMk2(CF), . . . , EMkn(CF)が生成される様子が示される。

【0039】図3は本実施形態の不正データコピー防止装置に用いられるデータ構造例を示す図である。同図には、図2で説明した各暗号化データが組み合わせられてデータ構造をなした様子が示されている。すなわち各マスター鍵で暗号化されたコピー管理フラグCFとデータ暗号鍵Dkのペア211が順次並べられマスター鍵暗号化部212が構成され、マスター鍵暗号化部212の後ろにEDk(Dk)であるディスク鍵暗号化部213が付加されている。そしてディスク鍵暗号化部213の後ろにEDk(データ)であるデータ本体214が設けられ、データ構造体215が構成されている。

【0040】なお、上記したように、データ本体214はデジタル化された文書、音声、画像あるいはプログラム等のデータが暗号化されたものであり、このデータ本体214にデータ暗号鍵Dk及びコピー管理フラグCFが含まれてなるデータ構造体215が、そのまま又はさらに加工された形で、DVD-RAM107やD-VCRに記憶され、また、ネットワーク等を介してSTB101に送られてくる。すなわち、このデータ構造体215の形で送信や記録媒体への記録によるユーザ配布、販売を行う。

【0041】そして、本発明は、このデータ構造体215に含まれているCF、すなわち暗号化されて外部からの攻撃に耐え得るコピー管理フラグCFを利用して、データのコピー管理(世代管理、複写回数管理)を行い、不正なコピーデータを有効に再生させないようにするのである。

【0042】以下、上記データ構造体215を扱うデジタル記録再生機器において、いかにしてデータ再生、データコピー等が行われるかについて具体的に説明する。図4は本実施形態の不正データコピー防止装置を用いたデジタル記録再生機器の構成例を示す図である。

【0043】同図においては、送信機器301としてDVD-RAM、受信機器302としてD-VCRを用い、両機器301, 302をIEEE1394ケーブル303で接続した場合を例にとって説明する。説明の都合上、送信機器301、受信機器302には送信受信用の構成のみを示すが、各機器には送信受信用の両構成が含まれている。また、送信機器301、受信機器302としては、図1に示したように種々の組み合わせた考えられるものである。

【0044】送信機器301は、IEEE1394チップ311と、DVD-RAM312からデータ構造体215の形で保存されるデータを読み出し、またデータ書

き込みを行う読出書込回路313とから構成されている。さらに、IEEE1394チップ311には、IEEE1394インターフェース処理を行い受信機器302と通信するIEEE1394I/F部314と、鍵共有回路315、暗号化回路316、CF変更部317が設けられている。

【0045】一方、受信機器302は、IEEE1394チップ321, 322と、再生データに画質調整等を施しIEEE1394チップ322を介してディスプレイ304にて表示させる表示処理部323と、IEEE1394チップ321のデータ再生コピー処理部334から出力されるデータ構造体215をDVカセット324に保存する書込処理部325と、DVカセット324からデータ構造体215を読み出してデータ再生コピー処理部334に入力する読出処理部326とによって構成されている。IEEE1394チップ321には、IEEE1394インターフェース処理を行い送信機器301と通信するIEEE1394I/F部331と、鍵共有回路332、復号化回路333、データ再生コピー処理部334が設けられている。

【0046】上記各構成のうち、鍵共有回路315, 332と、暗号化回路316と復号化回路333とは、データ構造体215をIEEE1394ケーブル303上で伝送させる際に、これを暗号化させるための構成である。

【0047】鍵共有回路315及び332は、IEEE1394ケーブル303での情報伝送により一時鍵Stkを安全に共有するようになっている。また、暗号化回路316は、CF変更部317から出力されたDVD-RAMデータ(データ構造体215)に対し鍵共有回路315からの一時鍵Stkを用いて暗号化を行う。さらに、復号化回路333は、鍵共有回路332からの一時鍵Stkを用い、IEEE1394I/F部331から受け取った暗号化されたデータ構造体215を復号してデータ再生コピー処理部334に引き渡すものである。なお、一時鍵Stkの鍵共有方式については、第4及び第5の実施形態でも詳しく説明する。

【0048】送信機器301のCF変更部317は、読出書込回路313で読み出されたデータ構造体215を暗号化回路316に引き渡すとともに、コピー管理フラグCFを変更し、そのCFの変更された新たなデータ構造体215でもってDVD-RAM312内の同一データ構造体を更新する。

【0049】受信機器302のデータ再生コピー処理部334は、復号化回路333又は読み出し処理部326から受け取ったデータ構造体215を自己のもつ鍵束Mksにより解読してデータ暗号鍵Dk及びコピー管理フラグCFを取り出すとともに、データ暗号のとかれたデータを表示処理部323に出力する。また、コピー管理フラグCFを変更したのち、自己のマスター鍵束Mksを用

いてデータ構造体215を作成し、書込み処理部325に保存用データ(コピーデータ)として出力する。

【0050】次に、以上のように構成された本発明の実施の形態に係る不正データコピー防止装置の動作について説明する。送受信間でデータ転送が行われることとなると、まず、送信機器301と受信機器302との間で、鍵共有回路315、332により一時鍵Stkの共有化が行われる。

【0051】次に、DVD-RAM312からデータ構造体215が読み出され、CF変更部317を介して暗号化回路316に入力され、ここでデータ構造体215の一時鍵Stkによる暗号化が行われる。そして、暗号化

EMk1 (Dk) , EMk2 (Dk) , ... , EMkn (Dk)	...215a
EMk1 (CF) , EMk2 (CF) , ... , EMkn (CF)	...215b
EDk(Dk)	; ディスク鍵暗号化部 ...213
EDk (データ)	; データ本体 ...214

にわけようになっている。EDk (データ) 以外は長さが決まっています、図3のごとくヘッダとして付加された部分をわけるとは容易である。

【0054】さて、マスター鍵束MknもしくはMksを暗号鍵として暗号化されたデータ暗号鍵215aは、図3のマスター鍵暗号化部212の一部であり、安全のためIEEE1394チップの利用者が勝手に取り出せない領域に記憶される。このマスター鍵束で暗号化されたデータ暗号鍵215aは、この装置製造メーカーに供給されているマスター鍵束Mksを順に復号鍵として用いて復号される。

【0055】このときEMk1 (Dk) , EMk2 (Dk) , ... , EMkn (Dk) 215aは、いったんメモリ402に取り込まれ、制御信号1にて受信機器のIEEE1394チップ内のマスター鍵束Mksを順に復号鍵として取り出し復号化回路403にて、例えばEMk1 (Dk) から順に復号していく。

【0056】復号して得られたDk' を復号鍵としてEDk(Dk)を復号化回路404にて復号してDk'' を得る。Dk' とDk'' とを判定回路405で比較する。Dk' =Dk'' であるならば、データ暗号鍵を暗号化するのに用いたマスター鍵と、暗号化されたデータ暗号鍵を復号するのに用いたマスター鍵とが等しいことに他ならない。しかしDk' ≠Dk'' であるならば、データ暗号鍵を暗号化するのに用いたマスター鍵と、暗号化されたデータ暗号鍵を復号するのに用いたマスター鍵とが異なっているということである。さらに全てのマスター鍵についてDk' ≠Dk'' ならば、この暗号、例えばEMk1 (Dk) は、このチップの所有するマスター鍵束Mksでは解けないということである。

【0057】このような場合には、制御信号2により次のEMk2 (Dk) をメモリ402から呼び出し、IEEE1394チップ内のマスター鍵束Mksを用いて、上記と同様の操作をDk' =Dk'' となるEMkiが見つかる

されたデータ構造体215はIEEE1394I/F部314によってIEEE1394ケーブル303を介して受信機器302に送信される。

【0052】一方、CF変更部317ではコピー管理フラグCFの変更が行われる。図5は本実施形態のCF変更部の構成及びその処理を示す図である。同図に示すように、DVD-RAM312から読み出されたデータ構造体215は、暗号化回路316に送出されるとともに、データ読み取り制御回路401に入力される。

【0053】データ読み取り制御回路401は、受け取ったデータ構造体215を

まで繰り返す。

【0058】Dk' =Dk'' となれば、そのときのマスター鍵でEMki (Dk) からデータ暗号鍵Dk が取り出したことになる。そこで制御信号3によりメモリ406に記憶されているEMk1 (CF) , EMk2 (CF) , ... , EMkn (CF) のうち、EMki (CF) を取り出す。なお、マスター鍵束で暗号化されたコピー管理フラグ215bは、1からn (又はs) まで、マスター鍵束で暗号化されたデータ暗号鍵215aと同じ並びになっているので、EMki (CF) の特定は容易である。

【0059】次に、復号化回路407により特定されたマスター鍵を用いたEMki (CF) の復号が行われCFが得られる。そしてCF変更回路408にてコピー管理フラグCFが変更されてデータ更新回路409の暗号化回路410に入力される。

【0060】このデータ更新回路409には、データ読み取り制御回路からEDk (データ) , すなわちデータ構造体215におけるデータ本体214が入力されるようになっている。一方、Dk , 変更されたCFも入力されるようになっており、暗号化回路410において、これらがマスター鍵束Mks及びデータ暗号鍵Dk によって暗号化され、データ本体214のヘッダとして付される。

【0061】このメーカー毎のマスター鍵束Mksで暗号化され、かつ変更されたコピー管理フラグCFを有するデータ構造体215 (MknがMksとなった他は、図3と同一構造) が読出書込回路313に出力され、この新たなデータ構造体でDVD-RAM312の対応する部分が更新される。

【0062】ここで、コピー管理フラグCFは世代管理情報と、コピー回数管理情報とからなっている。世代管理というのは、マスターディスクから子供コピー、さらに孫コピーを作るように新世代を作る場合のコピー管理である。一方、コピー回数管理というのは、そのデータ構造体で何回コピーを行ったかを管理するものである。

この場合、CF変更部317を通過して暗号化回路316に引き渡されたデータ構造体215はその受け取り先で世代管理がなされることとなり、一方、CF変更部317により、DVD-RAM312に戻され更新されるデータ構造体は、CF変更回路408にてコピー回数のみがカウントアップされて世代の変更は行われない。なお、カウント数が最大値となるとデータ送出先（受信機器302）において正常なデータコピーができなくなる。

【0063】このようにして、送信機器301においてコピー管理がなされる一方、受信機器301においても受信したデータ構造体215についてのコピー管理が行われる。以下、受信側での処理を説明する。

【0064】まず、受信機器302のIEEE1394 I/F部331で受け取った暗号化されたデータ構造体は、鍵共有回路332から与えられる一時鍵Skにより復号化回路333にて復号され、データ再生コピー処理部334に入力される。

【0065】図6は本実施形態のデータ再生コピー処理部の構成及びその処理を示す図であり、図5と同一部分には同一符号を付する。データ再生コピー処理部334に入力されるデータ構造体215は、まずデータ読取り制御回路401に入力され、図5のCF変更部317の場合と同様にわけられる。以下、判定回路405にてデータ暗号鍵Dkが取り出され、さらに、復号化回路407にてコピー管理フラグCFが取り出されるまでは、図5のCF変更部317と同様な処理が行われる。

【0066】次に、取り出されたコピー管理フラグCFの状態がCF判定回路411にて判定される。コピー管理フラグCFの世代管理及びコピー回数管理の具体的な内容は後述する。ここで、コピー管理フラグCFがこれ以上コピーできない世代にあるか否か、たとえば次世代コピーが許される世代であってもそのデータ構造体のコピー可能な最大回数に達しているか否かが判定されることで、コピー可否が判断される。そして、CF判定回路411によりコピー管理フラグCF及びコピー可否の判定結果（制御信号4）が鍵変更回路412に与えられる。

【0067】鍵変更回路412は、記録コマンドや再生コマンドあるいはその両方がユーザから入力されていることを知らせる制御信号5にて、コピー管理フラグCFと、先に得られたデータ暗号鍵Dkをそのままあるいは変更して出力するようになっている。

【0068】データ再生を行い、単にディスプレイ304に表示する場合には、データ構造体215のデータ本体214たるEDk（データ）が復号化回路413で復号化されてデータとして取り出されて表示処理部323に出力される。このとき、鍵変更回路412から復号化回路413には、常に判定回路405で取り出されたデータ暗号鍵Dkが復号化鍵として与えられる。したがって、正常なデータ暗号鍵Dkが取り出される限りは、コ

ピー管理フラグCFの状態にかかわらず、データ再生だけは正常に行われる。

【0069】これに対して、DVカセット324にデータコピーを行う場合には、CF判定回路411での判定結果によりその処理が異なることになる。まず、コピー管理フラグCFがコピー可能な状態にある場合について説明する。このときには、鍵変更回路412からは、コピー管理フラグCFがCF変更回路414に入力され、一方、データ暗号鍵Dkが暗号化対象データとしてかつ暗号化鍵としてコピー回路415の暗号化回路416に入力される。

【0070】CF変更回路414では、世代の変更が行われる。すなわちコピー管理フラグCFの世代管理情報が変更され、データ構造体が次世代のものとされる。この変更されたコピー管理フラグCFは、コピー回路415に入力される。

【0071】つまり、コピー回路415には、データ構造体のデータ本体214としてのEDk（データ）がデータ読取り制御回路401から入力され、さらにDk及び変更されたCFが入力されている。暗号化回路416では、Dk及びCFがマスター鍵束Mks及びデータ暗号鍵Dkによって暗号化され、データ本体214のヘッダとして付される。

【0072】このメーカ毎のマスター鍵束Mksで暗号化され、かつ変更されたコピー管理フラグCFを有するデータ構造体215（MknがMksとなった他は、図3と同一構造）が書込み処理部325に出力され、DVカセット324にコピーデータとして格納される。なお、このコピー操作でマスター鍵束がMknからMksとなっているので、以降、保存されたデータ構造体215は、このメーカ互換性がなくなり、マスター鍵束Mksをもたない機器では再生やコピーができなくなる。

【0073】また、この保存されたデータ構造体215を再生する場合には、読出処理部326からマスター鍵束Mksで暗号化されたデータ構造体がデータ読取り制御回路401に入力され、上記と同様な処理がなされる。

【0074】次に、コピー管理フラグCFがコピー可能な状態にない場合について説明する。このときデータ構造体はすでにコピーできない状態にあるので、CF変更回路414では特にコピー管理フラグCFの変更はなされない。一方、鍵変更回路412から暗号化回路416へのデータ暗号鍵の出力がコピー可能な場合とは異なったものとなる。

【0075】すなわちコピー不可の場合、鍵変更回路412は、暗号化対象データかつ暗号化鍵となるデータ暗号鍵として、判定回路405で取り出された正規のデータ暗号鍵Dkとは異なる偽のデータ暗号鍵Dk*を暗号化回路215に入力する。Dkを変更して偽のDk*を作るには、例えばDkのビットを反転するとか、ビットシフトを行うとか、ある特定の数値との排他論理和をとる

などの演算を行う、といった方法がある。

【0076】なお、各データを与えられたコピー回路415及び暗号化回路416の処理は上記と同様である。しかしながら、この回路415で生成され保存されたデータ構造体215においては、図3におけるEDk（データ）の暗号鍵はDkのままで、ヘッダ部であるマスター鍵暗号化部212及びディスク鍵暗号化部213に使用され格納されるデータ暗号鍵Dk*はすべてにせものとなっている。したがって、このデータ構造体を復号するときには、偽のデータ暗号鍵Dk*が取り出され、偽のデータ暗号鍵Dk*によるでたらめなデータ再生が行われることになる。

【0077】以上が送信機器301から受信機器302へデータ構造体215をコピーし、またデータ再生する場合の処理である。すなわち送信機器301で元データに対するデータコピーの回数管理が行われ、受信機器302にて受け取りデータをコピーすることによるデータコピーの世代管理が行われている。

【0078】次に、コピー管理フラグCFの具体的な内容及び世代管理、コピー回数管理について図7、図8を用いて説明する。図7はコピー管理フラグCFの構成例を示す図である。本実施形態では、8ビットを1バイトとして、上位3ビットをコピー世代の管理のためのビット（世代管理情報）とし、下位5ビットをコピー回数管理するためのビット（コピー回数管理情報）としている。

【0079】図8はコピー世代の管理ビットの状態遷移を表した図である。コピー世代管理ビットは、
000...コピー可能
001...子コピー可能（孫コピーは不可）→子は111になる
011...孫コピー可能（曾孫コピーは不可）→子は001になり、孫は111になる
111...コピー不可

とする。従って図8のごとく、コピー世代管理ビットがオール0の場合は、コピーをしてもオール0のままであるが、コピー世代管理ビットが“001”である場合は、子供のコピーは可能であるが、孫のコピーは不可としているため、コピーをすると子供のコピーのコピー世代管理ビットは“111”となり、コピー不可となる。一方、コピー世代管理ビットが“011”である場合は、孫コピーまで可能であるので、子供のコピーのコピー世代管理ビットは“001”となり、孫コピーのコピー世代管理ビットは“111”となってコピー不可となる。こうして、コピー世代を管理するものとする。

【0080】また、コピー回数は、コピー回数管理ビットが最大値になると、たとえコピー世代管理ビットがコピー可能な世代であってもコピー不可となる。本実施形態ではコピー回数管理ビットが5ビットであるため、1回から32回までの回数管理しかできないが、ビット数

を増やせば、さらに多くの回数管理が可能である。

【0081】回数管理の場合、例えばソフトウェアのマスターディスクのユーザ数を制限する場合などに利用が可能である。マスターディスクのコピー世代管理フラグは子供のコピーが可能な“001”としておく。こうすれば、ユーザがコピーしたソフトウェアを更にコピーされることを防ぐことが可能である。

【0082】コピー回数管理ビットは、マスターディスクからコピーできるユーザ数を表しており、本実施形態の場合、0～32人までコピーすることが可能である。例えば、マスターディスクからコピー可能なユーザ数を10人とする。この場合、最初のコピー回数管理ビットは“01010”である。一人がコピーすると、マスターディスクのCF： 00101001
ユーザのCF： 11100000
となり、ユーザがコピーしたソフトウェアは、他媒体へ記録ができなくなる。

【0083】こうして、10人のユーザがソフトウェアをコピーすると、マスターディスクのCF： 00100000
となり、子供のコピーが可能なままであるが、回数が0回であるため、これ以上のコピーは許可されない。

【0084】なお、最後の人がコピーをした時点でマスターディスクのコピー世代管理ビットを“111”にしておく方法もある。上述したように、本発明の実施の形態に係る不正データコピー防止装置及び方法は、コピー管理フラグCFを暗号化してデータ構造体215に含ませるようにしたので、コピー管理フラグCFを伝送途中で書き換えて不正コピーすることを防止でき、コピー管理フラグCFに対する不正者の攻撃を確実に防御できる。これにより著作権を確実に保護することができる。

【0085】また、データ再生コピー処理部334にCF判定回路411及び鍵変更回路412を設けてコピーできないデータ構造体をコピーするときには、データ暗号鍵を変更するようにしたので、不正なコピーデータを有効に再生させないようにすることができる。

【0086】また、CF変更部317を設けて、コピーのために伝送するデータ構造体のコピー回数をカウントアップさせることができ、きめ細かく効果的なコピー管理を実現することができる。

【0087】さらに、データ再生コピー処理部334にCF判定回路411及びCF変更回路414を設けてコピー対象となるデータ構造体の世代を進めるようにしたので、きめ細かく効果的なコピー管理を実現することができる。

【0088】また、鍵共有回路315、332及び暗号化回路316を設け、伝送されるデータ構造体を暗号化するようにしたので、受信側に復号化回路333を備えていなければ当該データを利用できないようにすることができる。また、機器間を一時的な暗号鍵で暗号化して

伝送を行うため、機器間を接続するケーブルから他記録媒体に記録して再利用する不正なコピーを防止することができる。

【0089】さらに、コピーが可能か否かを示すためのコピー管理フラグCFには、コピーが何世代まで可能かを示す部分と、コピー回数が何回まで可能かを示す部分とを設けたので、コピーの世代管理と回数管理により、きめ細かなコピー許可不許可管理を行うことができる。

【0090】なお、本実施形態では、CF変更部317、データ再生コピー処理部334は、それぞれIEE E1394チップ311、321に含まれる構成としたが、本発明はこのような構成に限られるものでなく、例えばCF変更部317、データ再生コピー処理部334が別チップとなる構成としてもよい。

(発明の第2の実施の形態) 本実施形態では、不正データコピー防止方法を実現するための他のデータ構造について説明する。

【0091】図9は本発明の第2の実施形態に使用されるデータ構造の構成方法を説明する図であり、図2と同一部分には同一符号を付して説明を省略する。図9においては、コピー管理フラグCFを暗号化する暗号化鍵にデータ暗号鍵Dkが用いられる他、各データの暗号化は第1の実施形態と同様である。ただし、図2ではマスター鍵束が使用される関係上、CFの暗号化データは複数となったが、本実施形態では、データ暗号鍵Dkが用いられるので、CFの暗号化データは1つである。

【0092】図10は本実施形態の不正データコピー防止装置に用いられる他のデータ構造例を示す図である。同図には、図9で説明した各暗号化データが組み合わされてデータ構造をなした様子が示されている。すなわちこのデータ構造体226では、データ暗号鍵Dkで暗号化されたコピー管理フラグ部221と、マスター鍵で暗号化されたデータ暗号鍵222が順次並べられたマスター鍵暗号化部223と、EDk(Dk)であるディスク鍵暗号化部224とが順次並べられヘッダ部となっている。そして、EDk(データ)であるデータ本体225の先頭に、このヘッダ部が設けられ、データ構造体226として構成されている。

【0093】このようなデータ構造体226は、データコピーのコピー管理、不正コピー防止を実現するべく不正データコピー防止装置を備えたデジタル記録再生機器において記録再生用データとして使用される。

【0094】その適用対象は、第1の実施形態で説明したデジタル記録再生機器と同様である。すなわち、データ構造体226は、データ読取り制御回路における振り分け対象が一部変更され、CFを暗号復号する鍵がDkになっている他は、図1、図4、図5、図6に示した各装置において利用できる。

【0095】なお、データ構造体226を用いた場合の図6に対応したデータ再生コピー処理部334bの構成

を図11に示す。図11は本実施形態の不正データコピー防止装置のデータ再生コピー処理部の構成及びその処理を示す図であり、図6と同一部分には同一符号を付する。なお、不正データコピー防止装置を含むシステムの全体構成は図4に示す場合と同様である。

【0096】同図において、第1の実施形態(図6)との相違点は、データ読取り制御回路401にデータ構造体226が入力され、そのデータ振り分けにより、EDk(CF)をメモリ406に入力しマスター鍵暗号化部223をデータ本体225とともにコピー回路415bに入力することと、復号化回路407で使用する復号化鍵が、判定回路405で得られたデータ暗号鍵Dkとなっていることと、また、コピー回路415bにおいては各部からの入力により、データ構造体215ではなくデータ構造体226を生成することである。なお、コピー回路415bにおいてはデータ読取り制御回路401から入力されたマスター鍵暗号化部223がデータ構造体226のヘッダ部の一部にそのまま利用される。なお、コピー不可時にDkがDk*に変更された場合、EDk*(Dk*)となる新たなディスク鍵暗号化部224のDk*がDkと異なっているので、このデータ構造体のマスター鍵暗号化部223からデータ暗号鍵Dkが取り出されることはない。

【0097】この結果、コピー回路416から出力されるデータ構造体226は、CFが変更されあるいは不正コピー時にDk*が変更される他、データ再生コピー処理部334bに入力されたデータ構造体226のままである。特にマスター鍵暗号化部223がメーカ毎のマスター鍵束Mksで置き換えられることがないので、コピーされたデータはメーカ互換性を失うことはない。

【0098】なお、本実施形態で使用される送信側のCF変更部も、上記図6～図11間と同様な変更が図5に示すCF変更部317に施される(図示せず)。すなわち復号化回路407に復号鍵としてデータ暗号鍵Dkが入力され、データ更新回路409にマスター鍵暗号化部223が入力されて更新用のデータ構造体226のヘッダ部に利用される。したがって、コピー回数管理時においてもデータ構造体226はメーカ互換性を失わない。

【0099】上述したように、本発明の実施の形態に係る不正データコピー防止装置及び方法は、第1の実施形態と同様な構成を設けた他、デジタルデータとしてデータ構造体226を使用するようにしたので、第1の実施形態と同様な効果が得られる他、データコピーを行う際に、最初のマスター鍵束Mknで暗号化されたデータ暗号鍵をそのまま残すことができ、コピーデータやコピー元のデータのメーカ互換性を失わないようにすることができる。

(発明の第3の実施の形態) 第1又は第2の実施形態では、図3に示すデータ構造体215又は図10に示すデータ構造体226のみがシステムで使用される場合につ

いて説明した。しかし、実際の使用においては、これらの各データ構造体が混在する場合も考えられる。本実施形態では、このような場合の対応方法について説明する。

【0100】図12は本発明の第3の実施形態の不正データコピー防止装置に用いられる他のデータ構造例を示す図である。同図(a)は、データ構造体215の先頭に識別ビット231aを付加し、データ構造体215bとしたものを示す。

【0101】一方、同図(b)は、データ構造体226の先頭に識別ビット231bを付加し、データ構造体226bとしたものを示す。データ再生コピー処理部334、334b、CF変更部317(第2実施形態の場合を含む)のデータ読取り制御回路401は、この識別ビット231a、231bを読み取って、各部に何れのデータ構造体に対応した処理を行うかの制御信号を出力する。

【0102】上述したように、本発明の実施の形態に係る不正データコピー防止装置及び方法は、第1又は第2の実施形態と同様な構成を設けた他、デジタルデータとしてデータ構造体215b及び226bを使用するようにしたので、第1又は第2の実施形態と同様な効果が得られる他、異なる形式のデータ構造体を混在させても、それぞれのデータ構造に応じた処理を行うことができる。

(発明の第4の実施の形態) 上記各実施形態では、データ構造体をいかなる構成とし、これに含まれるコピー管理フラグCFによりいかにしてデータコピー管理を行うかについて説明してきた。しかしながら、上記方法でデータコピー管理を行ってもデータ伝送路上でデータ構造体を不正に取得され、いわゆるデータ横流しをされてしまったのでは、上記データ管理方法の効果も減じることになる。これを防止すべく、上記各実施形態では、鍵共有回路315、332を設け、一時鍵Stkを共有してこの一時鍵Stkで暗号化されたデータを伝送路(IEEE1394ケーブル303)上で伝送させるようにしている。

【0103】本実施形態及び第5の実施形態では、この一時鍵Stkを共有する方法について説明する。したがって、本実施形態及び第5の実施形態で以下に説明される鍵共有システムが第1、第2又は第3の実施形態における鍵共有回路315、332に用いられることになる。

【0104】図13は本発明の第4の実施形態におけるマスター鍵束を利用した各機器間で一時暗号鍵を共有するための仕組みを説明した図であり、ネットワークまたはケーブルにより接続された機器間においてネットワークまたはケーブル上を流れる秘密情報を暗号化/復号化するための一時鍵の共有方法について図示したものである。本実施形態では、IEEE1394で接続された送信機器と受信機器との間で一時鍵を共有する場合につい

て説明する。

【0105】同図において、送信機器501と受信機器503とがIEEE1394ケーブル502によって接続されている。送信機器にマスター鍵の鍵束504a

(Mks)が記録され、受信機器にマスター鍵の鍵束504b(Mks)が記録されている。両者の鍵束は異なっても構わないが、必ず鍵束の中の何個かは同じマスター鍵が含まれている必要がある。本実施形態では、両者のマスター鍵の鍵束(Mks)は同じであるものとする。

【0106】送信機器501の鍵共有にかかる部分は、一時鍵生成回路505と暗号化回路507a、507bによって構成される。一時鍵生成回路505は、ネットワークまたはケーブル上を流れるデータを一時的に暗号化するための一時鍵を生成するものである。この一時鍵生成回路505は、例えば特定の長さの乱数を生成する乱数発生器で行うことが好ましい。

【0107】一時鍵506(Sk)は一時鍵生成回路505で生成された鍵である。暗号化回路507aは、マスター鍵の鍵束504aの何れかで一時鍵506を暗号化する回路で、暗号化回路107bは一時鍵Skを一時鍵Skで暗号化する。暗号化回路507aと暗号化回路507bは暗号化方式が同じであれば同一の回路で構成しても構わない。EMki(Sk)508は暗号化回路507aの出力で、ESk(Sk)509は507b暗号化回路の出力である。

【0108】一方、受信機器503の鍵共有にかかる部分は、復号化回路510a、510bと一時鍵判定回路513によって構成される。復号化回路510aは、暗号化回路507aの出力をマスター鍵の鍵束Mkiで復号する。復号化回路510bは、暗号化回路507aの出力を復号回路510aの出力で復号する。

【0109】Ska511は復号回路510aの出力で、Skb512は510b復号回路の出力である。一時鍵判定回路513は復号化回路510aの出力と復号化回路510bの出力とを比較判定する判定回路である。制御信号514は判定の結果によりマスター鍵の鍵束を変更するための信号で、Sk515は判定の結果得られた一時鍵である。

【0110】次に、以上のように構成された本発明の実施の形態に係る一時鍵共有装置の動作について説明する。まず、もしマスター鍵が1つだけ存在するのであれば(これをMk0とする)、単に送信機器501にてMk0でSkを暗号化し、このEMk(Sk)を受信機器503へ送り、受信機器503にてMk0でEMk(Sk)を復号化することにより、Skを取り出すことができる。しかし、万一マスター鍵が破れた(漏洩した)場合、マスター鍵を交換しなければならず、新しい機器と古い機器とで互換性がなくなる可能性がある。

【0111】そこで本実施形態では、複数のマスター鍵からなる鍵束Mksのうちの使用したマスター鍵Mkiを直

接的に指し示す識別情報は送信機器501から受信機器503へは送らず、その代わりに、上記マスター鍵Mkiを特定可能とする情報（ここではEMki(Sk)508及びESk(Sk)509を意味する）を送信機器501から受信機器503へ送り、受信機器503にてSkの暗号化に使用されたマスター鍵Mkiがマスター鍵のうちのいずれかであるかを特定するとともに、このマスター鍵の特定を通じてSkを得る。

【0112】図14は本実施形態の動作を説明する流れ図である。まず、送信機器501において、受信機器503との間で共有される一時鍵506が一時鍵生成回路505で生成される(S11)。

【0113】以下、図14のステップS12のより詳しい手順について説明する。生成されたSkはn個のマスター鍵（共通鍵暗号方式における共通鍵）の鍵束504aのうちから例えばランダムあるいは順番に選んだ1つ（これをMkiとする）で暗号化される。すなわちMks(s=1, ..., n; nは2以上の整数)のうちいずれか1つのMkiで一時鍵Skを暗号化回路507aで暗号化してEMki(Sk)を得る。

【0114】このマスター鍵Mksはあらかじめ登録されているものであり、ユーザは見るできない仕組みになっている。なお万一、マスター鍵が破られたことが発覚した場合、それ以降、送信機器にはその破られたものを除いてマスター鍵が作り込まれる。受信機器503側は、その破られたものを除いてマスター鍵が作り込まれてもよいし、そうしなくてもよい。ただし、IEEE1394の場合、どの機器が送信機器となるか受信機器となるか、区別がない(D-VCRやDVD-RAMなどの録画再生機器は、送信機器と受信機器とになりうる)ため、破られたマスター鍵を除いたものに換えることが望ましい。なお、全体の制御は図示しない各機器内の制御部が司るものとする。制御部は、例えばプログラムを各機器内に内蔵されたCPUなどで実行することにより実現することができる。

【0115】さらに、暗号化回路507bによりSk自身を暗号鍵として用いてSkを暗号化してESk(Sk)を得る。そして、EMki(SK)とESk(Sk)を、IEEE1394ケーブル502を通じて受信機器503へ送る。

【0116】次に、受信機器503にて、まずマスター鍵を1つ選ぶ（これをMkpとする）。選んだMkpを復号鍵として、復号化回路510aにより復号化し、 $DMkp(EMki(Sk)) = Ska$ を得る。

【0117】次に、復号化回路510aからの出力Skaを復号鍵として復号化回路510bにより、 $ESk(Sk)$ を復号化し、 $DSka(ESk(Sk)) = Skb$ を得る。

【0118】次に、一時鍵判定回路513により、SkaとSkbとが一致するか否かを調べる。ここで、送信機器501にてSkを暗号化したマスター鍵MkiがMkpであったならば、

$$Ska = DMkp(EMki(Sk)) = Sk$$

となり、従って、

$$Skb = DSka(ESk(Sk)) = DSk(ESk(Sk)) = Sk$$

となり、ゆえに、

$$Ska = Skb = Sk$$

となる。

【0119】つまり、一時鍵判定回路513により、SkaとSkbとが一致することが判った場合には、 $Mki = Mkp$ 、かつ、 $Ska = Skb = Sk$ であり、この場合、一時鍵判定回路513は $Ska = Skb = Sk$ を出力する。

【0120】一方、一時鍵判定回路513により、SkaとSkbとが一致しないことが判った場合には、 $Mki \neq Mkp$

であり、送信機器501にてSkはこのMkpで暗号化されておらず、それ以外のマスター鍵で暗号化されたことがわかる。この場合、一時鍵判定回路513は出力をしないか、あるいは一時鍵判定回路513の出力は以後の処理部へ伝えられない。

【0121】以降は、SkaとSkbとが一致するまで、復号化に用いるMkpを変更して、上記の手順を繰り返す。例えば、最初にMkpとMk1を用いて上記の手順を行ってSkaとSkbとが一致しなかった場合に、次にMk2へと更新して再び上記の手順を繰り返すのである。

【0122】以上のような手順を用いて、送信機器501にてどのマスター鍵を用いたのかを受信機器503で特定できるとともに、送信機器501と受信機器503との間で一時鍵Skを安全に共有することが可能となる。

【0123】上述したように、本発明の実施の形態に係る不正データコピー防止装置及び方法は、第1、第2又は第3の実施形態と同様な構成を設けた他、マスター鍵を用いて送信機器501と受信機器503との間で一時鍵Skを安全に共有することができるようにしたので、第1、第2又は第3の実施形態と同様な効果が得られる他、機器間を接続するケーブルから他記録媒体に記録して再利用する不正なコピーをより一層確実に防止することができる。

(発明の第5の実施の形態) 本実施形態では、一時鍵を共有する他の方法、すなわちマスター鍵を用いずに一時鍵を共有する方法について、図15と図16を用いて説明する。

【0124】この方式は、「日経エレクトロニクス、No. 676, pp. 13-14, 1996. 11. 1

8」に開示された技術を応用したものである。図15は本発明の第5の実施形態における鍵共有回路の構成例を示すブロック図である。

【0125】図16はこの鍵共有回路によりマスター鍵束を用いずに各機器間で一時暗号鍵を共有するための仕組みを説明した図である。いま、IEEE1394で接続された機器にノードが割り振られ、図16に示すようにノード#1とノード#2とで一時鍵を共有するものとする。まず図15を用いて、本実施形態における鍵共有手順に用いる鍵共有回路630a、630bの構成について説明する。

【0126】鍵共有回路630aは、チャレンジ鍵生成回路631a、認証鍵生成回路633a、比較回路635a、一時鍵生成回路637aを備えている。同様に鍵共有回路630bは、チャレンジ鍵生成回路631b、認証鍵生成回路633b、比較回路635b、一時鍵生成回路637bを備えている。

【0127】チャレンジ鍵生成回路631a、631bは、例えば乱数生成アルゴリズムを用いて、生成の都度変化するチャレンジ鍵を生成する。認証鍵生成回路633a、633bは、例えば一方向性関数を用いて、チャレンジ鍵から認証鍵を生成する。

【0128】比較回路635a、635bは、2つの認証鍵が一致するかどうか比較する。一時鍵生成回路637a、637bは、例えば一方向性関数を利用して、2つの認証鍵から一時鍵を生成する。

【0129】認証鍵生成回路633aと認証鍵生成回路633bは、例えば同一のアルゴリズムを用いることにより、同一のチャレンジ鍵に対して同一の認証鍵を生成するものとする。

【0130】一時鍵生成回路637aと一時鍵生成回路637bは、例えば同一のアルゴリズムを用いることにより、同一の2つの認証鍵から同一の一時鍵を生成するものとする。

【0131】次に、図15、図16を参照しながら鍵共有の手順について説明する。まず、鍵共有手段のフェイズ1では、ノード2にて、チャレンジ鍵生成回路631aによりチャレンジ鍵(challenge Key)CK1を生成し、これをノード#1に伝える。

【0132】次に、ノード#2の認証鍵生成回路633aとノード#2の認証鍵生成回路633bのそれぞれにて、チャレンジ鍵CK1をもとに認証鍵(key1)K1を生成し、またノード#1からノード#2へ生成した認証鍵K1を転送する。

【0133】そしてノード#2にて、比較回路635aによりノード#2とノード#1のそれぞれで生成された2つの認証鍵K1を比較する。もし一致すれば次のフェイズ2に移行する。もし一致しなければ異常終了となる。

【0134】次に、フェイズ2では、ノード#1にて、

チャレンジ鍵生成回路631bによりチャレンジ鍵(challenge Key)CK2を生成し、これをノード#2に伝える。

【0135】次に、ノード#1の認証鍵生成回路633bとノード#2の認証鍵生成回路633aのそれぞれにて、チャレンジ鍵CK2をもとに認証鍵(key2)K2を生成し、またノード#2からノード#1へ生成した認証鍵K2を転送する。

【0136】そしてノード#1にて、比較回路635bによりノード#1とノード#2のそれぞれで生成された2つの認証鍵K2を比較する。もし一致すれば次のフェイズ3に移行する。もし一致しなければ異常終了となる。

【0137】そして、フェイズ3では、ノード#2の一時鍵生成回路637aとノード#1の一時鍵生成回路637bのそれぞれにて、認証鍵K1と認証鍵K2をもとに一時鍵(BUS Key)すなわち一時鍵(Skt)を生成する。

【0138】これによって、ノード#1とノード#2との間で安全に一時鍵Sktが共有化される。上述したように、本発明の実施の形態に係る不正データコピー防止装置及び方法は、第1、第2又は第3の実施形態と同様な構成を設けた他、マスター鍵を用いずに送信機器と受信機器の間で一時鍵Skを安全に共有することができるようにしたので、第1、第2又は第3の実施形態と同様な効果が得られる他、機器間を接続するケーブルから他記録媒体に記録して再利用する不正なコピーをより一層確実に防止することができる。

【0139】なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。また、各実施形態に記載した手法は、計算機に実行させることができるプログラムとして、例えば磁気ディスク(フロッピーディスク、ハードディスク等)、光ディスク(CD-ROM、DVD等)、半導体メモリ等の記憶媒体に格納し、また通信媒体により伝送して頒布することもできる。本装置を実現する計算機は、記憶媒体に記録されたプログラムを読み込み、このプログラムによって動作が制御されることにより上述した処理を実行する。

【0140】

【発明の効果】以上詳記したように本発明によれば、第1の目的は、データ内のコピー管理を行う部分に対する不正者の攻撃を確実に防御できる不正データコピー防止装置及び方法並びに記録媒体を提供することができる。

【0141】また、本発明によれば、不正なコピーデータを有効に再生させないようにする不正データコピー防止装置及び方法を提供することができる。さらに、本発明によれば、きめ細かなコピー管理を実現できる不正データコピー防止装置及び方法を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る不正データコピー防止装置を適用するデジタル記録再生機器の接続構成例を示すブロック図。

【図2】同実施形態に使用されるデータ構造の構成方法を説明する図。

【図3】同実施形態の不正データコピー防止装置に用いられるデータ構造例を示す図。

【図4】同実施形態の不正データコピー防止装置を用いたデジタル記録再生機器の構成例を示す図。

【図5】同実施形態のCF変更部の構成及びその処理を示す図。

【図6】同実施形態のデータ再生コピー処理部の構成及びその処理を示す図。

【図7】コピー管理フラグCFの構成例を示す図。

【図8】コピー世代の管理ビットの状態遷移を表した図。

【図9】本発明の第2の実施形態に使用されるデータ構造の構成方法を説明する図。

【図10】同実施形態の不正データコピー防止装置に用いられる他のデータ構造例を示す図。

【図11】同実施形態の不正データコピー防止装置のデータ再生コピー処理部の構成及びその処理を示す図。

【図12】本発明の第3の実施形態の不正データコピー防止装置に用いられる他のデータ構造例を示す図。

【図13】本発明の第4の実施形態におけるマスター鍵束を利用した各機器間で一時暗号鍵を共有するための仕組みを説明した図。

【図14】同実施形態の動作を説明する流れ図。

【図15】本発明の第5の実施形態における鍵共有回路の構成例を示すブロック図。

【図16】鍵共有回路によりマスター鍵束を用いずに各機器間で一時暗号鍵を共有するための仕組みを説明した図。

【符号の説明】

211…マスター鍵で暗号化されたコピー管理フラグCFとデータ暗号鍵Dkのペア

212…マスター鍵暗号化部

213…ディスク鍵暗号化部

214…データ本体

215…データ構造体

221…コピー管理フラグ部

222…データ暗号鍵

223…マスター鍵暗号化部

224…ディスク鍵暗号化部

225…データ本体

226…データ構造体

301…送信機器

302…受信機器

303…IEEE1394ケーブル

311, 321, 322…IEEE1394チップ

314, 331…IEEE1394I/F部

315, 332…鍵共有回路

316…暗号化回路

401…データ読み取り制御回路

402, 406…メモリ

403, 404, 407, 413…復号化回路

405…判定回路

408…CF変更回路

409…データ更新回路

410, 416…暗号化回路

411…CF判定回路

412…鍵変更回路

414…CF変更回路

415…コピー回路

501…送信機器

502…IEEE1394ケーブル

503…受信機器

504a, 504b…マスター鍵束

505…一時鍵生成回路

506…一時鍵

507a, 507b…暗号化回路

510a, 511b…復号化回路

513…一時鍵判定回路

630a, 630b…鍵共有回路

631a, 631b…チャレンジ鍵生成回路

633a, 633b…認証鍵生成回路

635a, 635b…比較回路

637a, 637b…一時鍵生成回路

CF…コピー管理フラグ

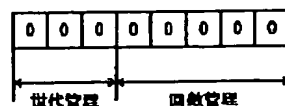
Dk…データ暗号鍵

Mkn…マスター鍵束

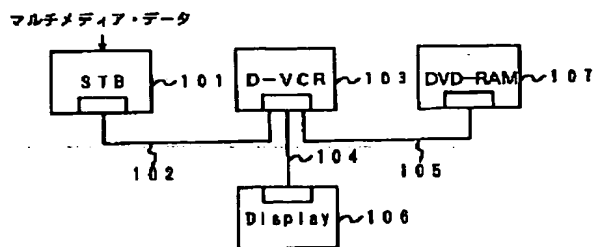
Mks…各メーカーに付与されたマスター鍵束

Stk…一時鍵

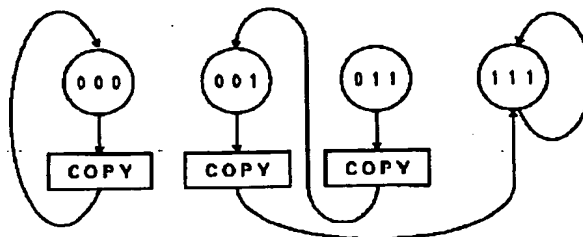
【図7】



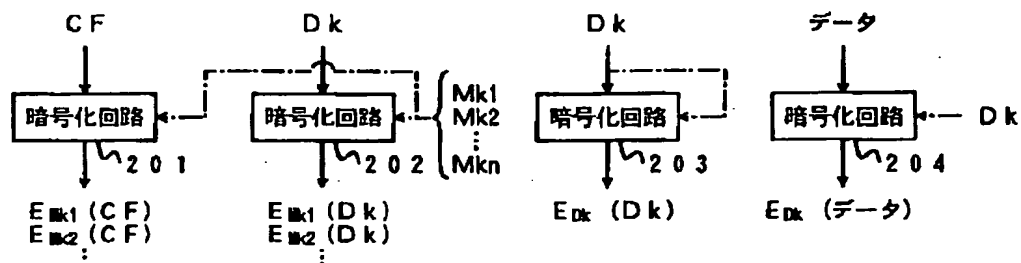
【図1】



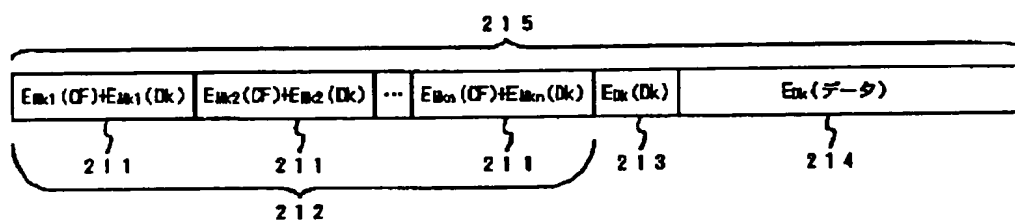
【図8】



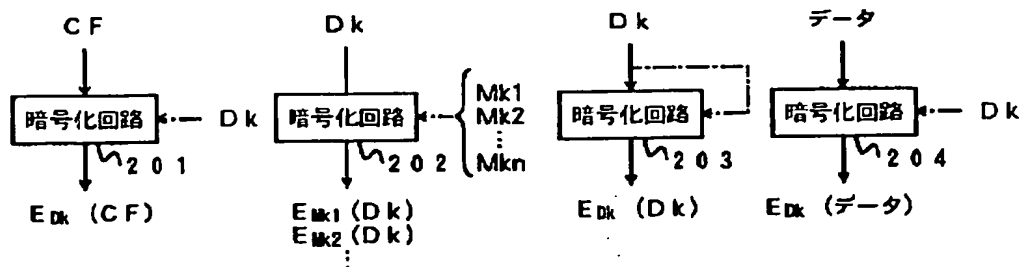
【図2】



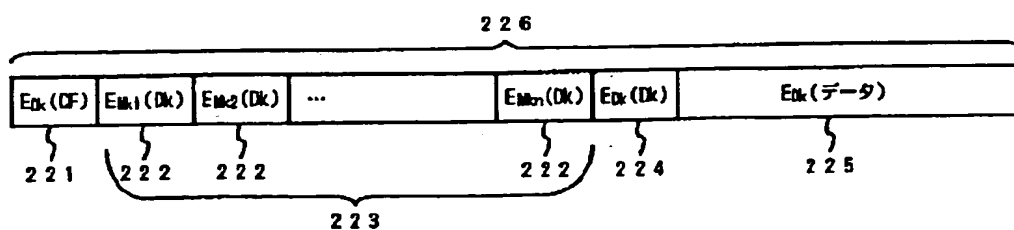
【図3】



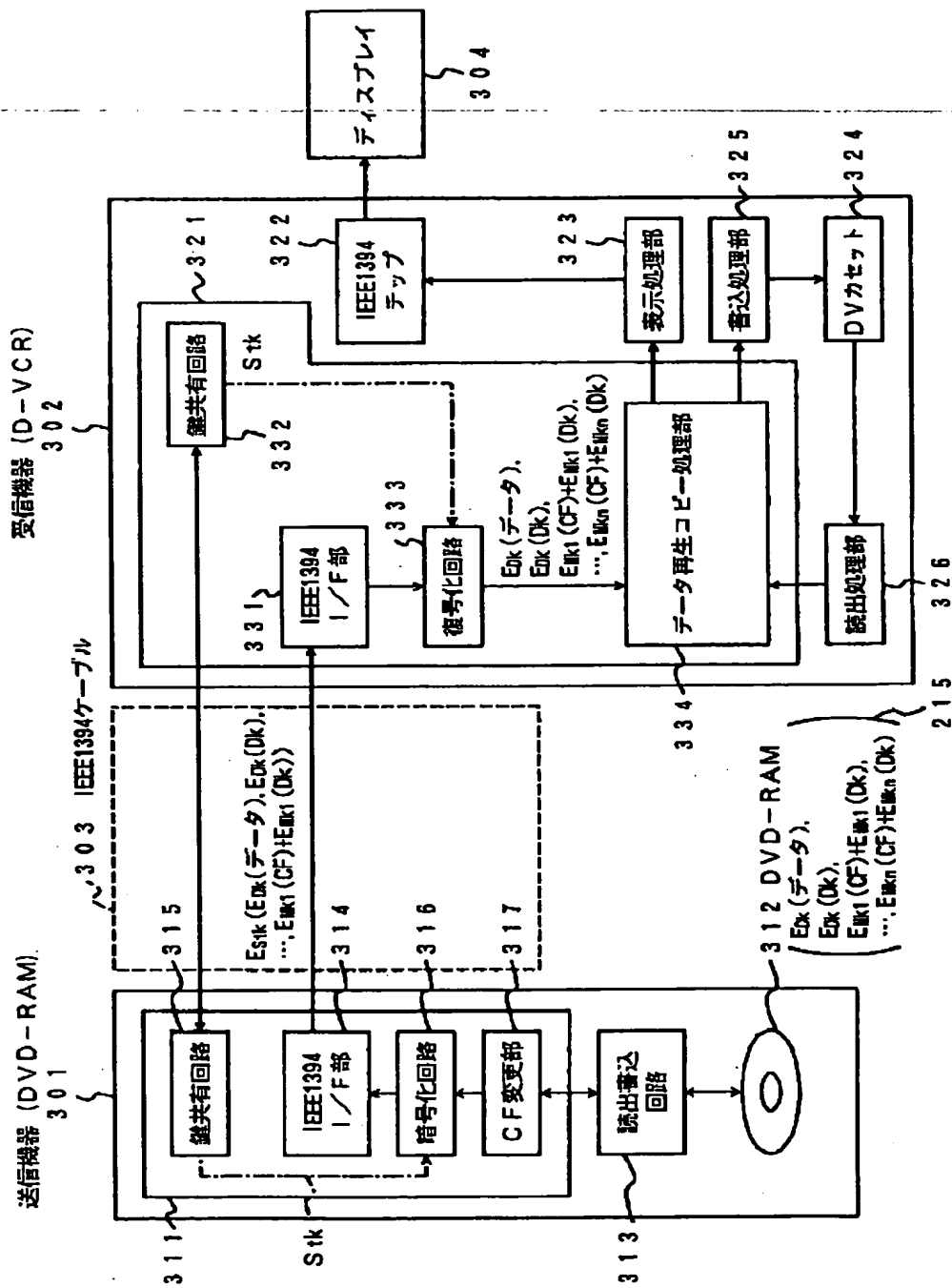
【図9】



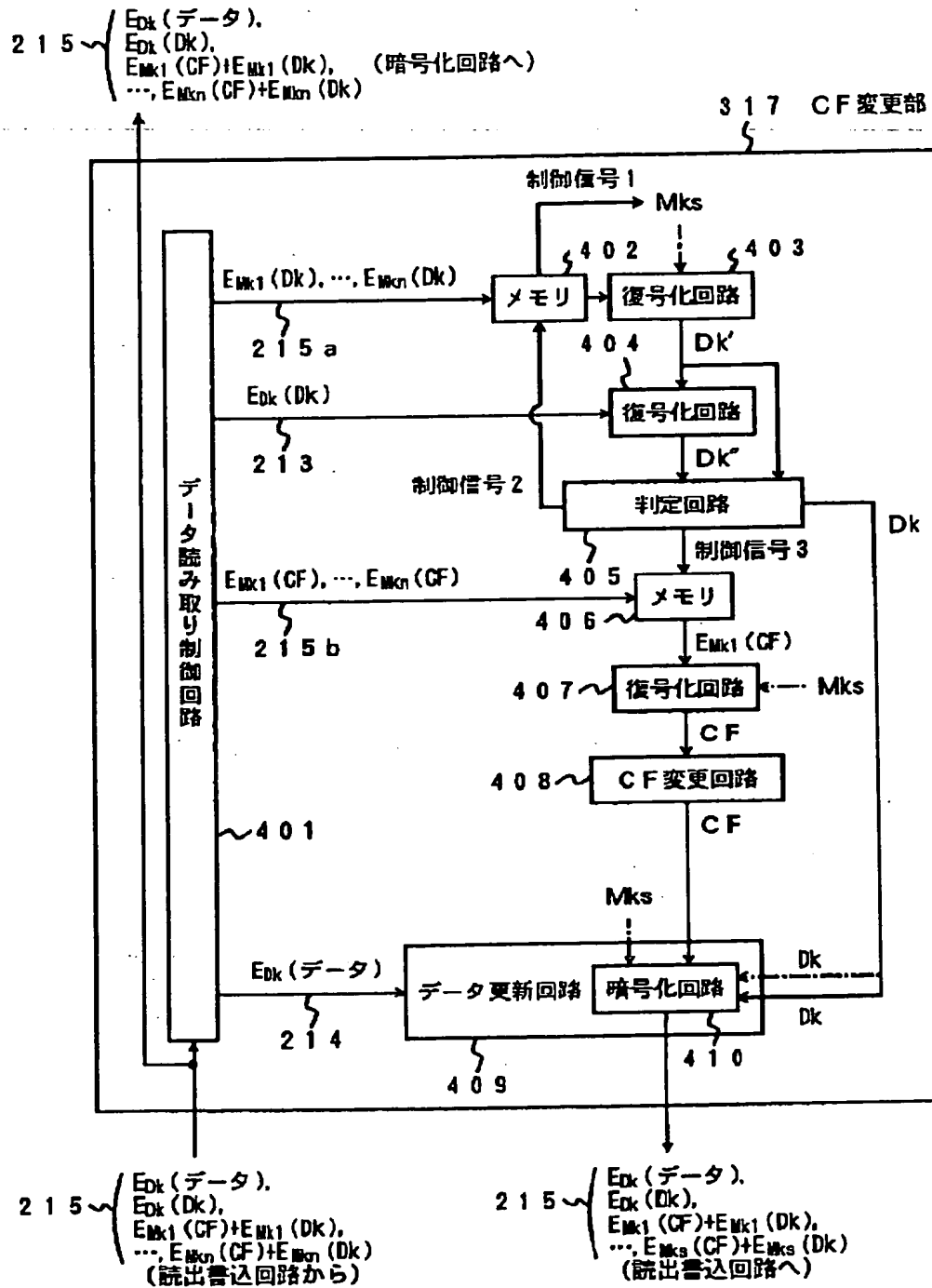
【図10】



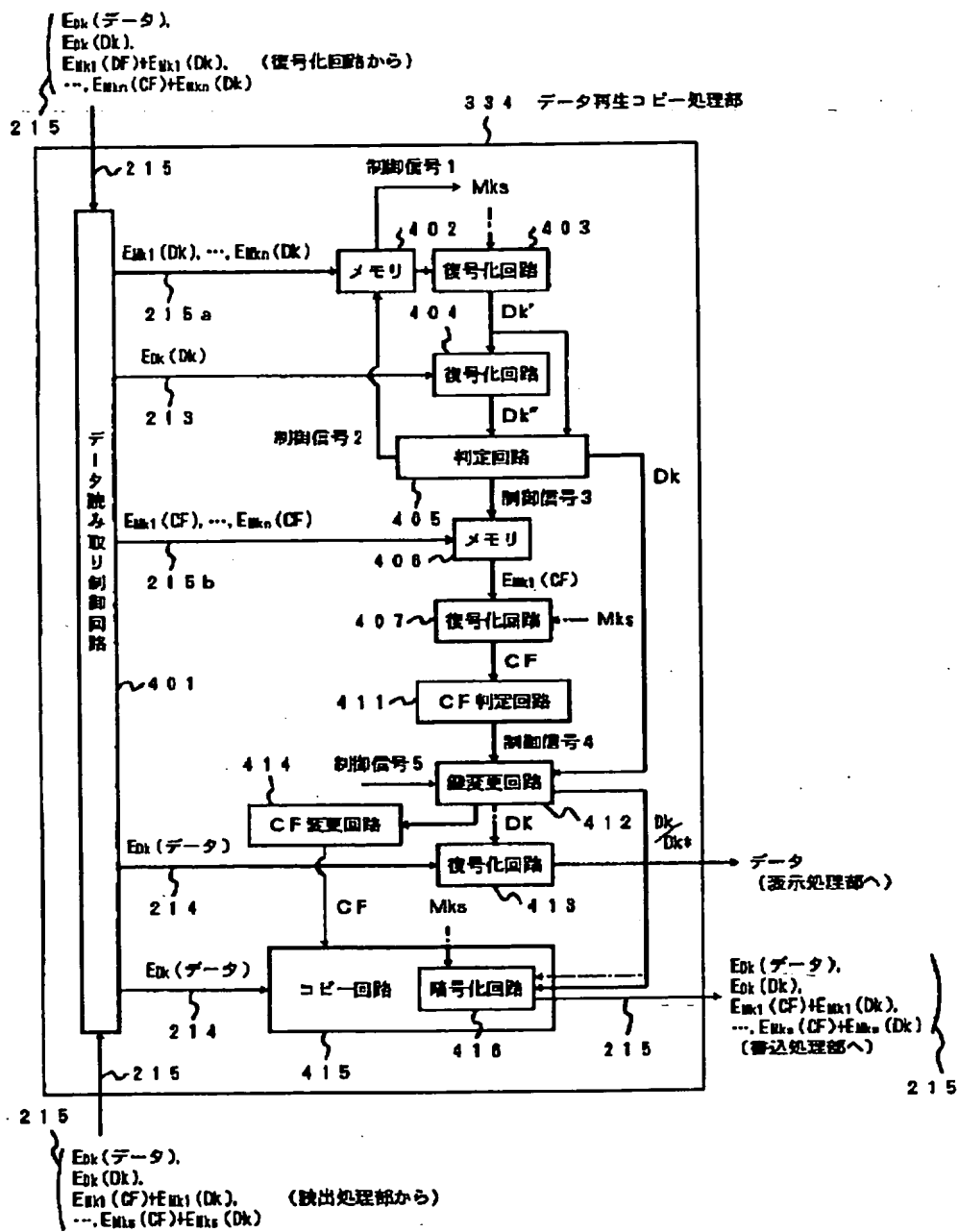
【図4】



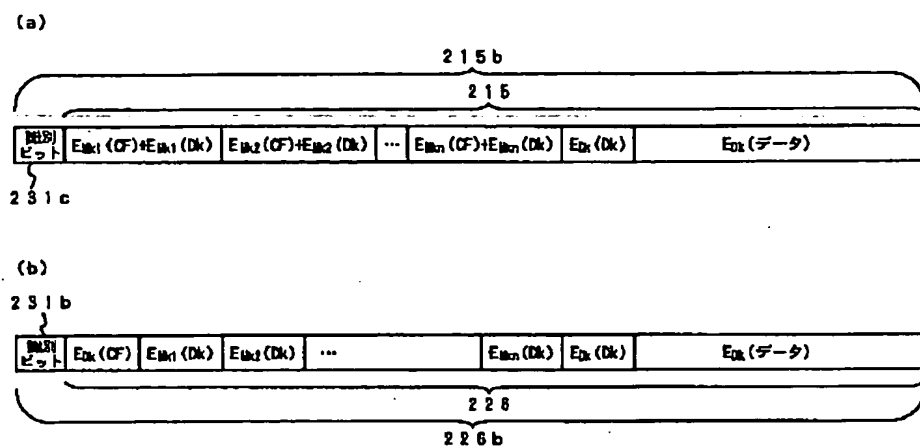
【図5】



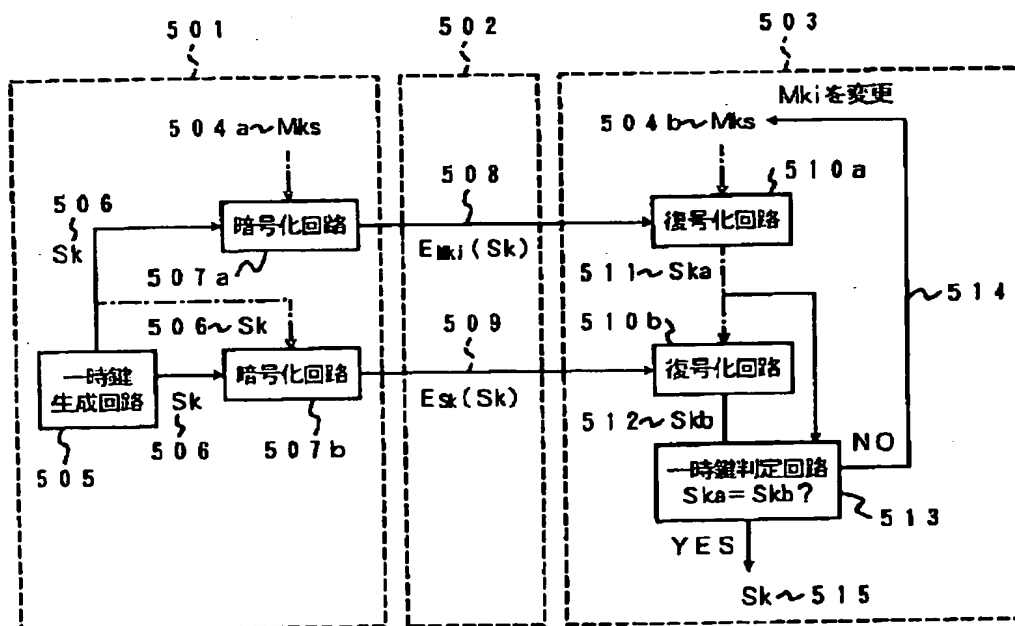
【図6】



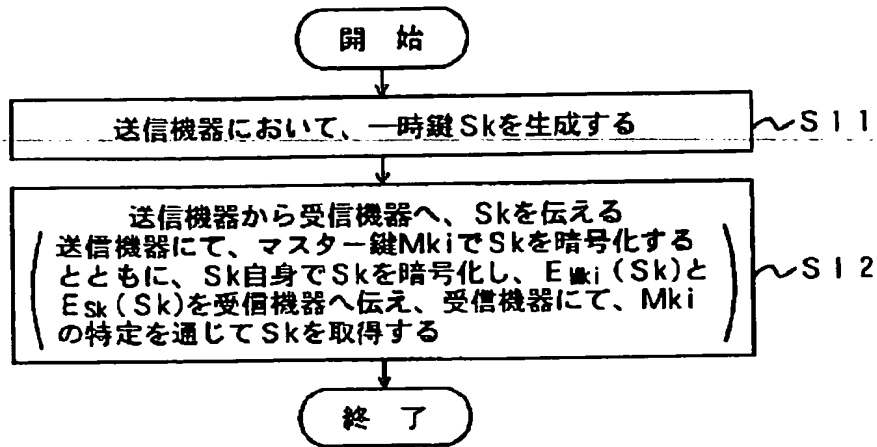
【図12】



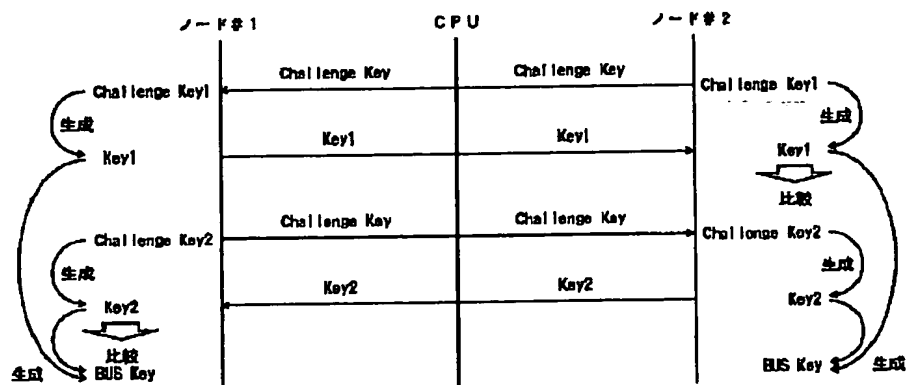
【図13】



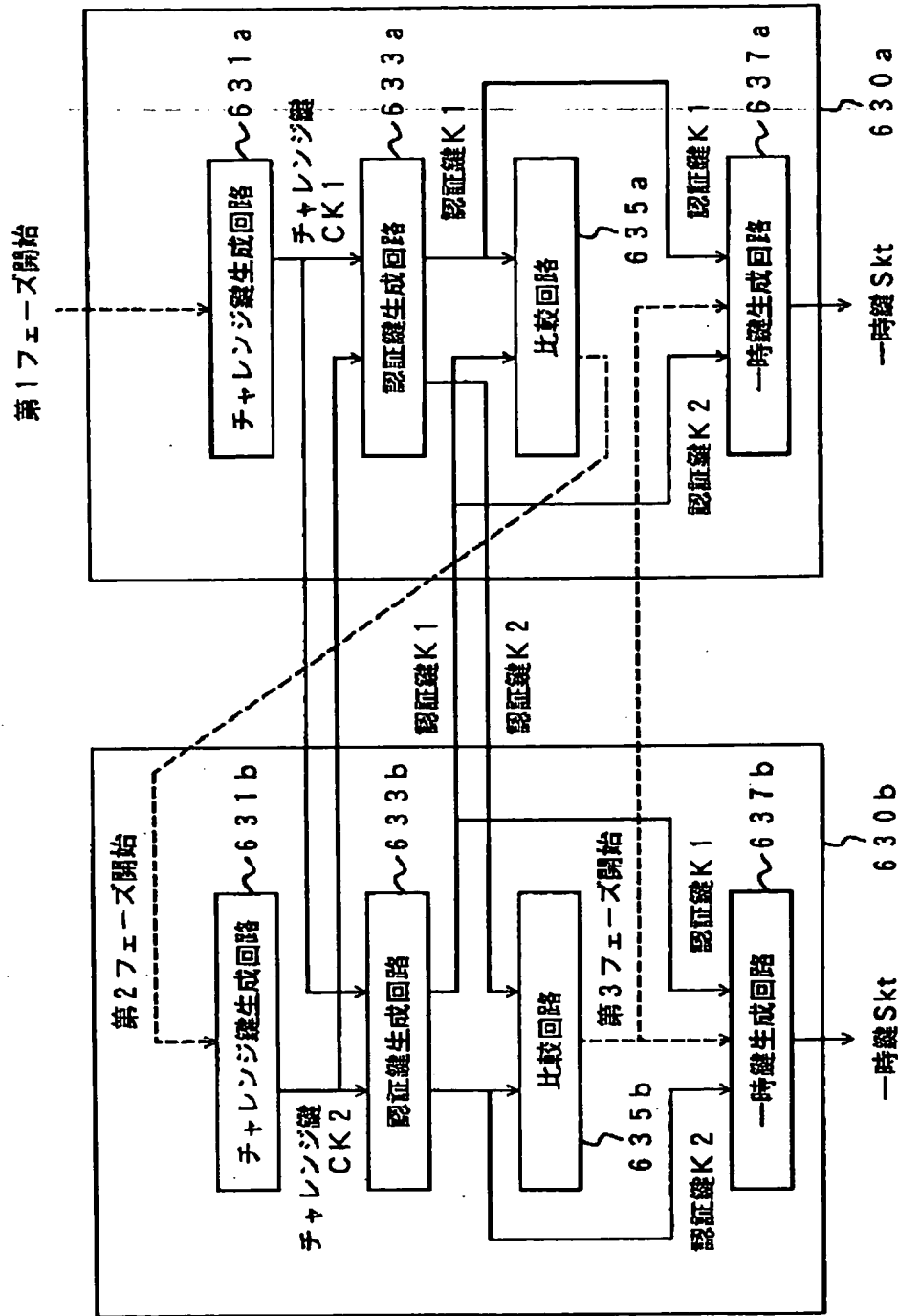
【図14】



【図16】



【図15】



フロントページの続き

(51)Int.Cl.⁶
H04L 9/36

識別記号

FI
H04L 9/00

685